

EXHIBIT 655

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN**

AUTHENTICOM, INC., Plaintiffs, v. CDK GLOBAL, LLC, and THE REYNOLDS AND REYNOLDS COMPANY, Defendants.	No. 3:17-CV-318-JDP
--	---------------------

**DEFENDANT THE REYNOLDS AND REYNOLDS COMPANY'S
INITIAL DISCLOSURES**

Pursuant to Federal Rule of Civil Procedure 26(a)(1), The Reynolds and Reynolds Company (“Reynolds”) makes the following initial disclosures. These disclosures are based on information reasonably available to Reynolds as of this date. Continuing investigation and discovery may alter these disclosures and/or identify other potential witnesses and documents. Reynolds reserves the right to supplement and amend these disclosures.

Nothing in these disclosures shall be construed as an admission or acceptance by Reynolds of the relevance or admissibility of any witness, document, or fact in these disclosures. Nothing in these disclosures shall be construed as a waiver of the attorney-client privilege, attorney work-product doctrine, or any other applicable privilege, protection, or doctrine. Reynolds reserves the right to object to the testimony of any of the witnesses identified herein and to the production or introduction into evidence of any document within the categories set forth herein on the basis of privilege, relevance, or any other applicable objection.

These disclosures are made only for the purpose of this action.

All of the disclosures below are subject to the above limitations, objections, and qualifications.

I. **The name and, if known, the address and telephone number of each individual likely to have discoverable information—along with the subjects of that information—that the disclosing party may use to support its claims or defenses, unless solely for impeachment.**

Pursuant to Rule 26(a)(1)(A)(i), and to the best of Reynolds' knowledge, the following individuals are likely to have discoverable information that Reynolds may use to support its claims or defenses:

A. Persons subject to Authenticom's control

Steven Cottrell, Chief Executive Officer

Mr. Cottrell has knowledge of Authenticom's efforts to circumvent Reynolds' security protocols, Authenticom's attempts to solicit dealers' login credentials in violation of their contracts with Reynolds, Authenticom's security and privacy measures, Authenticom's data distribution and data scraping technology and policies, Authenticom's security measures (or lack thereof), Authenticom's finances, and the other matters on which he testified at the preliminary injunction hearing.

Brian Clements, Chief Operations Officer

Mr. Clements has knowledge of Authenticom's efforts to circumvent Reynolds' security protocols, Authenticom's attempts to solicit dealers' login credentials in violation of their contracts with Reynolds, Authenticom's security and privacy measures (or lack thereof), and Authenticom's data distribution and data scraping technology and policies.

Noah La Liberte, General Manager

Mr. La Liberte has knowledge of Authenticom's efforts to circumvent Reynolds' security protocols, Authenticom's attempts to solicit dealers' login credentials in violation of their contracts with Reynolds, Authenticom's security and privacy measures (or lack thereof), and Authenticom's data distribution and data scraping technology and policies.

All current and former employees, consultants, and principals of Plaintiff Authenticom who:

- Have knowledge of or participated in the accessing of Reynolds' DMS without Reynolds' authorization;
- Have knowledge of Authenticom's cybersecurity and data privacy policies, protocols, and practices;

- Have knowledge of the software and other techniques that Authenticom uses to pull, scrape, or push data in or out of the Reynolds DMS, including any efforts or attempts to circumvent Reynolds' security protocols;
- Have knowledge of Authenticom's DealerVault technology and practices; or
- Have knowledge of Authenticom's 2014 loan commitment.

All parties subject to Authenticom's control will be contacted through counsel for Authenticom.

B. Persons subject to Reynolds' control

Robert Schaefer

Vice President of Data Services

Mr. Schaefer has knowledge related to Reynolds' data security policies, the reasons for those policies, Reynolds' efforts over time to enforce and implement those policies, Authenticom's efforts to circumvent them, and the other matters on which he testified at the preliminary injunction hearing.

Kelly Hall

Senior Vice President of Software Development

Mr. Hall has knowledge of the harm and losses caused by hostile, third party access to Reynolds' DMS; Reynolds' efforts to stop such access; the Reynolds' DMS architecture; and the benefits to Reynolds, its customers, and consumers of having a closed architecture.

Ron Lamb

Immediate Past President and former Senior Vice President of Sales

Mr. Lamb has knowledge regarding the DMS market, the applications market, competition between DMS competitors, Reynolds' efforts to compete in the DMS market, dealers' DMS purchasing decisions, and other DMS providers' products.

Reynolds-affiliated witnesses should be contacted through counsel for Reynolds.

C. Persons subject to Defendant CDK Global ("CDK")'s control

Howard Gardner

Mr. Gardner has knowledge of CDK's rationale for entering into the 2015 agreements with Reynolds and the other matters on which he testified at the preliminary injunction hearing.

Malcolm Thorne

Mr. Thorne has knowledge of CDK's decision to launch its Security First initiative and the other matters on which he testified at the preliminary injunction hearing.

CDK-affiliated witnesses will be contacted through counsel for CDK.

D. Other third parties

Bryan D. Anderson, Former President of DealerVault, LLC

Mr. Anderson has knowledge of Authenticom's efforts to circumvent Reynolds' security protocols, Authenticom's attempts to solicit dealers' login credentials in violation of their contracts with Reynolds, Authenticom's security and privacy measures (or lack thereof), Authenticom's data distribution and data scraping technology and policies, Authenticom's security measures (or lack thereof), Authenticom's finances, Authenticom's loan on which it bases its argument of harm, and other matters relevant to the issues raised by Authenticom's claims and Reynolds' counterclaims.

Russell Gentry, Former President of DealerVault, LLC

Mr. Gentry may have knowledge of Authenticom's efforts to circumvent Reynolds' security protocols, Authenticom's attempts to solicit dealers' login credentials in violation of their contracts with Reynolds, Authenticom's security and privacy measures (or lack thereof), Authenticom's data distribution and data scraping technology and policies, Authenticom's security measures (or lack thereof), and Authenticom's finances.

Steve Dolezel, former Authenticom shareholder

Mr. Dolezel may have knowledge of Authenticom's business model, Authenticom's security and privacy measures (or lack thereof), Authenticom's finances, Authenticom's loan on which it bases its argument of irreparable harm, and Authenticom's use of that loan's proceeds to purchase Mr. Dolezel's interest in Authenticom.

Travis Robinson, former Authenticom shareholder

Mr. Robinson may have knowledge of Authenticom's business model, Authenticom's security and privacy measures (or lack thereof), Authenticom's finances, Authenticom's loan on which it bases its argument of irreparable harm, and Authenticom's use of that loan's proceeds to purchase Mr. Robinson's interest in Authenticom.

Cox Automotive

Cox Automotive has knowledge of competition within the DMS market and the application market, Cox's efforts to compete with Reynolds using its DealerTrack DMS product, and the design of Cox's DMS product (including its Open Track functions).

Peter C. Cassat

Vice President and General Counsel

Cox Automotive, Inc.

6205 Peachtree Dunwoody

Atlanta, GA 30328

T: 404-568-5678

Carfax, Inc.

Carfax has knowledge of its receipt and usage of data from Authenticom, dealership authorizations of data to be shared with Carfax, and other aspects of the data syndication process.

iHeartMedia, Inc.

iHeartMedia has knowledge of its DMS data polling solicitation and authorization process, including its requests for account credentials and IP addresses; its efforts to secure that information (or lack thereof); and other aspects of the data syndication process.

Other current or former Authenticom customers who have knowledge of their authorization from dealers to receive data, the data that they need to perform services for those dealers, the data that they receive from Authenticom, the security and privacy measures (or lack thereof) used to protect that data, and other aspects of the data syndication process.

Data Software Services, LLC (dba eLead)

eLead has knowledge of other DMS providers' and Reynolds' response to a data security breach caused by a rogue eLead employee; Reynolds' security practices and investigation into the data security incident; knowledge of eLead confidential documents provided by Plaintiff in this litigation; and benefits of being an RCI participant.

Penske Automotive

Penske has knowledge of Reynolds' refusal to authorize the creation of user IDs for Authenticom.

BMO Harris Bank N.A.

BMO Harris Bank has knowledge of Authenticom's finances and loan, and its intent and decision-making with respect to any potential foreclosure or refinancing of Authenticom's existing loan.

4106 State Road 93
Eau Claire, WI 54701

RCI Partners

Application vendors who participate in RCI may have knowledge of the value of RCI participation, the RCI certification process, their ability to use Authenticom for other data polling functions, the advantages of RCI integration over data scraping, and other knowledge regarding RCI.

Reynolds Dealer Customers

Dealerships who license Reynolds' DMS may have knowledge regarding Reynolds DMS access policies, the types of data stored in their DMS, the tools in the Reynolds DMS that allow for data reporting and extraction, and other knowledge regarding usage of Reynolds system.

Where possible, Reynolds has provided contact information for all applicable third parties above. All others are subject to ongoing investigation. References to "Authenticom" herein includes both Authenticom and DealerVault, as applicable. Reynolds further designates and incorporates here by reference all individuals identified in any other party's Rule

26(a)(1)(A)(i) disclosures. Reynolds reserves all rights to supplement the foregoing list through ongoing investigation and discovery, as well as for all rebuttal purposes.

II. A copy—or a description by category and location—of all documents, electronically stored information, and tangible things in the possession, custody or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment.

Reynolds previously produced documents in support of its defenses in connection with the preliminary injunction hearing. All parties already possess the February 2015 agreements, Reynolds DMS agreement, and RCI agreement that form the alleged basis for Authenticom's claims. Consistent with the Federal Rules, Reynolds will provide to Authenticom all other documents Reynolds may use to support its claims and defenses as they are identified, which may include, but are not limited to, the following categories:

1. Documents related to Reynolds' data security practices and policies and the reasons for those practices and policies;
2. Documents demonstrating Reynolds' efforts to enforce and implement its data security practices and policies;
3. Documents demonstrating Authenticom's efforts to circumvent Reynolds' data security practices and policies;
4. Documents demonstrating the harm caused by Authenticom's (and others') efforts to circumvent Reynolds' data security practices and policies;
5. Documents demonstrating the categories of testimony identified in Section I above.

Reynolds' documents are principally located in Dayton, Ohio and Houston, Texas. Reynolds reserves the right to supplement or amend this Initial Disclosure, if necessary, at a later time, or to supplement it through the course of discovery in this proceeding.

III. A computation of any category of damages claimed by the disclosing party, making available for inspection and copying under Rule 34 the documents or other evidentiary material, not privileged or protected from disclosure, on which such computation is based, including materials bearing on the nature and extent of injuries suffered.

Reynolds intends to pursue counterclaims for damages (together with equitable relief) under the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030; the Wisconsin Computer Crimes Act (“WCCA”), Wis. Stat. § 943.70(2)(a); the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; and Wisconsin common law. Depending on what Reynolds learns through discovery, it may seek damages under additional statutory and/or common law claims or seek to add additional liable parties. Discovery has not yet commenced and a substantial part of the information upon which Reynolds’ damages computations will be based is exclusively within the possession, custody, and control of Authenticom. Such damages are also partially dependent upon Authenticom’s actions during the time period in which this litigation progresses. Reynolds is entitled to a monetary judgment consisting of direct and consequential damages in an amount to be proven at trial, including but not limited to losses and damage caused to Reynolds and Reynolds’ DMS by Authenticom’s access and attempted access to Reynolds’ DMS, and lost revenue and damage to goodwill and business reputation caused by Authenticom’s conduct. Reynolds is further entitled to a monetary judgment for its costs, expenses, and reasonable attorneys’ fees incurred connection with this litigation as a result of Authenticom’s conduct. Reynolds will promptly supplement this response in accordance with the Federal Rules of Civil Procedure as additional information becomes available. Reynolds’ computation of damages will also be based on expert reports and analysis that have not yet been performed.

IV. For inspection and copying under Rule 34 any insurance agreement under which any person carrying on an insurance business may be liable to satisfy

part or all of a judgment which may be entered in the action or to indemnify or reimburse for payments made to satisfy the judgment.

Reynolds is not aware of any such insurance agreements.

DATED: August 31, 2017

Respectfully submitted,

John S. Skilton
JSkilton@perkinscoie.com
Charles G. Curtis, Jr.
CCurtis@perkinscoie.com
Michelle M. Umberger
MUUmberger@perkinscoie.com
Brandon M. Lewis
BLewis@perkinscoie.com
Jesse J. Bair
JBair@perkinscoie.com
PERKINS COIE LLP
One East Main Street, Suite 201
Madison, WI 53703
Telephone: 608-663-7460
Facsimile: 608-663-7499

Kathleen A. Stetsko
KStetsko@perkinscoie.com
PERKINS COIE LLP
131 South Dearborn St., Suite 1700
Chicago, IL 60603
Telephone: 312-324-8400
Facsimile: 312-324-9400

/s/ Aundrea K. Gulley
Aundrea K. Gulley
agulley@gibbsbruns.com
Brian T. Ross
bross@gibbsbruns.com
Brice A. Wilkinson
bwilkinson@gibbsbruns.com
Ross M. MacDonald
rmacdonald@gibbsbruns.com
GIBBS & BRUNS, LLP
1100 Louisiana, Suite 5300
Houston, Texas 77002
Telephone: 713-650-8805
Facsimile: 713-750-0903

Michael P.A. Cohen
MCohen@sheppardmullin.com
Amar S. Naik
ANaik@sheppardmullin.com
SHEPPARD MULLIN RICHTER & HAMPTON LLP
Suite 100
2099 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
Telephone: 202-747-1900
Facsimile: 202-747-1901

*Attorneys for Defendant
The Reynolds and Reynolds Company*

CERTIFICATE OF SERVICE

I hereby certify that on this 31st day of August, 2017, I caused a true and correct copy of the foregoing Reynolds' Initial Disclosures to be served on all counsel of record via email.

/s/ Aundrea K. Gulley
Aundrea K. Gulley

